PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-258059
(43)Date of publication of application : 21.09.2001

(51)Int.Cl. H04Q 7/22
H04Q 7/28
H04L 12/28

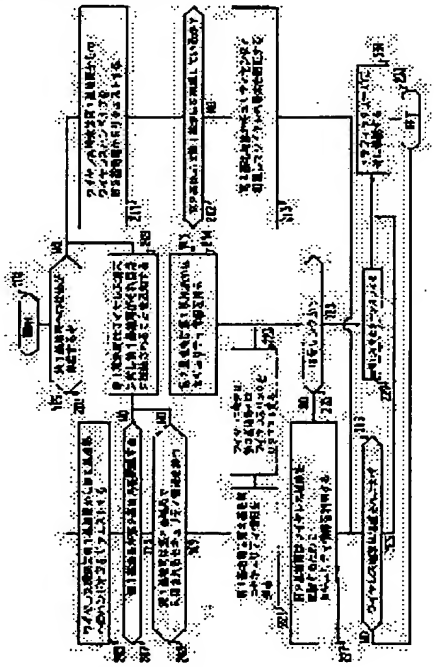
(21)Application number : 2001-029555
(22)Date of filing : 06.02.2001

(71)Applicant : LUCENT TECHNOL INC
(72)Inventor : DAVIES STEPHEN WILLIAM
VANDERVEEN MICHAELA C

(30)Priority
Priority number : 2000 501168 Priority date : 09.02.2000 Priority country : US

(54) EXECUTION METHOD FOR HANDS-OFF PROCEDURE IN NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for reducing the installation cost of a network by simplifying the architecture of the network.
SOLUTION: The method where hands-off procedure in a network having 1st and 2nd base stations and a wireless mobile terminal is executed, is characterized in that the method includes a step (A), where a request of hand-off from the 1st base station to the 2nd base station is received from the mobile terminal and a step (B), where the 1st base station transmits security information to the 2nd base station.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－258059
（P2001－258059A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
H04Q 7/22		H04L 12/28	300Z
7/28			310
H04L 12/28	300	H04Q 7/04	K
	310	H04B 7/26	107

審査請求　未請求　請求項の数22　ＯＬ　（全９頁）

(21)出願番号　特願2001－29555(P2001－29555)

(22)出願日　平成13年２月６日(2001.2.6)

(31)優先権主張番号　０９／５０１１６８

(32)優先日　平成12年２月９日(2000.2.9)

(33)優先権主張国　米国（ＵＳ）

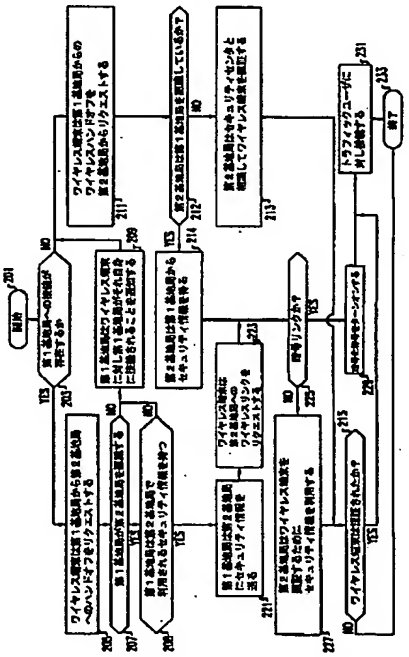
(71)出願人　596077259
ルーセント　テクノロジーズ　インコーポレイテッド
Ｌｕｃｅｎｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
アメリカ合衆国　07974　ニュージャージー、マレーヒル、マウンテン　アベニュー　600－700

(74)代理人　100081053
弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】　ネットワーク内のハンドオフの実行方法

(57)【要約】
【課題】効率的なネットワーク内のハンドオフの実行方法を提供する。
【解決手段】　本発明によれば、第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、（Ａ）第１基地局から第２基地局へのハンドオフのリクエストを移動端末から受信するステップと、（Ｂ）前記リクエストの応答して、第１基地局から第２基地局にセキュリティ情報を転送するステップと、を有することを特徴とする。



1

【特許請求の範囲】

【請求項１】　第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

（Ａ）第１基地局から第２基地局へのハンドオフのリクエストを移動端末から受信するステップと、

（Ｂ）前記リクエストの応答して、第１基地局から第２基地局にセキュリティ情報を転送するステップと、を有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項２】　前記セキュリティ情報は、少なくともランダム数と、第１基地局、第２基地局ではなく移動端末から得られた認証情報とキーとをからなる組を含むことを特徴とする請求項１記載の方法。

【請求項３】　前記セキュリティ情報の少なくとも一部を用いて、前記第２基地局への移動端末を有効にすることを特徴とする請求項１記載の方法。

【請求項４】　前記セキュリティ情報は、前記第１基地局が受信したセキュリティ情報のすべてではなく、前記リクエストに応答して、前記第１基地局から第２基地局に転送されることを特徴とする請求項１記載の方法。

【請求項５】　前記第１基地局が受信したセキュリティ情報の全ては、ワイヤレス移動端末の認証システムから受領することを特徴とする請求項４記載の方法。

【請求項６】　前記第１基地局が受領したセキュリティ情報の全ては、第３基地局から受領することを特徴とする請求項４記載の方法。

【請求項７】　前記（Ｂ）のステップは、（Ｂ）ステップを実行する前に第１基地局が第２基地局を認識しているときのみ行われることを特徴とする請求項１記載の方法。

【請求項８】　（Ｃ）前記第１基地局とワイヤレス端末が暗号化リンクを用いて通信しているときに、第２基地局とワイヤレス端末との間に暗号化リンクを初期化するステップを有し、

前記第２基地局は、第２基地局とワイヤレス端末との間の暗号化リンクを初期化する際に、前記第１基地局から第２基地局へ転送されたセキュリティ情報を用いることを特徴とする請求項１記載の方法。

【請求項９】　第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

（Ａ）第１基地局から第２基地局へのハンドオフのリクエストを、ワイヤレス端末から送信するステップと、

（Ｂ）前記第２基地局が第１基地局とのハンドオフに関連する旨のリクエストを受領する前に、第２基地局が第１基地局を認識しているときに、前記ワイヤレス端末で応答を受領するステップと、

（Ｃ）ユーザトラフィック用のワイヤレス端末を第２基地局に接続するステップとを有することを特徴とするネットワーク内のハンドオフの実行方法。

2

【請求項１０】　前記実行されたハンドオフは、前記第１基地局から第２基地局へ転送されたワイヤレス端末に関する情報を用いることを特徴とする請求項９記載の方法。

【請求項１１】　前記情報はセキュリティ情報であることを特徴とする請求項１０記載の方法。

【請求項１２】　前記情報はセキュリティセンタから受領したセキュリティ情報であることを特徴とする請求項１０記載の方法。

【請求項１３】　前記情報は、前記第１基地局と第２基地局以外の第３基地局から受領したセキュリティ情報であることを特徴とする請求項１０記載の方法。

【請求項１４】　前記情報はセキュリティ情報であり、（ｉ）パスワードと、（ｉｉ）チャレンジ－応答対と、（ｉｉｉ）チャレンジ－応答暗号化キーtupleからなる組からの少なくとも１つを含むことを特徴とする請求項１０記載の方法。

【請求項１５】　前記情報は基地局間の通信用のネットワークを介して受領したセキュリティ情報であることを特徴とする請求項１０記載の方法。

【請求項１６】　前記（Ｃ）ステップは、

前記第１基地局とワイヤレス端末が、ハンドオフリクエストの前に暗号化リンクを用いて通信しているときに、前記第２基地局とワイヤレス端末との間の暗号化リンクを初期化するステップを有し、

前記第２基地局は、前記第２基地局とワイヤレス端末との間の暗号化リンクを初期化する際に、前記レスポンスの一部として第１基地局から第２基地局へ転送されたセキュリティ情報を用いることを特徴とする請求項１０記載の方法。

【請求項１７】　第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

（Ａ）第１基地局から第２基地局へのハンドオフのリクエストを、ワイヤレス端末から送信するステップと、

（Ｂ）前記リクエストを受領する前に、第２基地局が第１基地局を認識していなかった場合には、第１基地局から与えられる情報を利用することなく、ワイヤレス端末が第２基地局に接続されなければならないという指示をワイヤレス端末で受領するステップを有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項１８】　前記情報はセキュリティ情報であることを特徴とする請求項１７記載の方法。

【請求項１９】　前記情報はセキュリティセンタから受領したセキュリティ情報であることを特徴とする請求項１７記載の方法。

【請求項２０】　前記情報は、前記第１基地局と第２基地局以外の第３基地局から受領したセキュリティ情報であることを特徴とする請求項１７記載の方法。

【請求項２１】　第１と第２の基地局とワイヤレス移動端末とを有するネットワーク内のハンドオフを実行する方法において、

（Ａ）第１基地局と第２基地局との間のハンドオフのリクエストをワイヤレスから第２基地局が受領するステップと、

（Ｂ）前記リクエストを受領する前に、第２基地局が第１基地局を認識しているときには、容易なハンドオフを実行するステップと、

（Ｃ）前記リクエストを受領する前に、第２基地局が第１基地局を認識していなかった場合には、容易でないハンドオフを実行するステップと、を有することを特徴とするネットワーク内のハンドオフの実行方法。

【請求項２２】　前記（Ｂ）のステップは、前記第１基地局から第２基地局へセキュリティ情報を転送するステップを含むことを特徴とする請求項２１記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はワイヤレス通信に関し、特に、ワイヤレス通信サービスを提供するネットワークの認定されたユーザのみがネットワークへのアクセスを許されるようなシステムに関する。

【０００２】

【従来の技術】従来のワイヤレスシステムは、認定されたワイヤレス端末のみがワイヤレスネットワークにアクセスすることができる。ワイヤレス端末がネットワークへアクセスできるようにするために、ワイヤレス端末は認定（認証）されなければならない。ここで本明細書において用語「認定（認証）」は、権限があると主張するエンティティを証明（認証）するプロセスである。電話の呼が持続する間、例えば呼が開始され、その後ワイヤレス端末がネットワーク内の規定された境界で移り変わるごとに、複数回認証が必要とされる。

【０００３】認証は、ワイヤレス内に登録された秘密情報から抽出された情報と、ネットワーク内のそれ以外の場所にある情報から抽出された情報とを比較することにより行われる。通常、比較する位置に最も近い場所にある抽出された情報の記憶場所からの一度の呼の間に、特定のワイヤレス端末に対して新たな認証が必要とされるごとに、この抽出された情報は送信される。

【０００４】ワイヤレスは基地局とエアリンクを介して通信される。基地局が比較場所にない場合には、基地局はワイヤレス端末から情報を比較場所に送らなければならない。抽出された情報が登録されているネットワーク内の場所は、いわゆるビジターロケーションレジスタ（visitor location register：ＶＬＲ）である。この抽出された情報は、いわゆるホームロケーションレジスタ（home location register：ＨＬＲ）、あるいは別の認証センタ（特定のネットワークのデザインによっては）で生成される。ワイヤレス端末が第１のＶＬＲによりサービスされる領域を、第２のＶＬＲによりサービスされる領域と区別するようなネットワーク境界に近づくにつれて、第１ＶＬＲは、抽出された情報を第２ＶＬＲに送信する。別の構成として第２ＶＬＲは、ＨＬＲからそれ自身で抽出した情報を得る。ＨＬＲは、ＨＬＲにより直接サービスされる領域でワイヤレス端末が最初に電源が入れられたときには、ＶＬＲとして機能する。

【０００５】好ましくないことに、様々な特殊なエンティティが存在し、複雑な制御手順が必要とされるために、従来のネットワークのコストは高かった。

【０００６】

【発明が解決しようとする課題】本発明の目的は、ネットワークのアーキテクチャーを単純化し、ネットワークの接地コストを低減する方法を提供する。

【０００７】

【課題を解決するための手段】前記課題を解決するために本発明は、ネットワーク内の規定された境界を基地局レベルまで押し下げることにより達成できる。しかしそうした結果は、ワイヤレス端末がある基地局から別の基地局へ通信を切り替えるごとに認証が必要とされることになる。言い換えると、規定された境界を基地局レベルまで押し下げた後、ある基地局から別の基地局へワイヤレス端末のハンドオフが存在するごとに、ネットワーク境界をまたぎ、認証が必要とされる。このような認証を効率的の個なうために、本発明によれば、セキュリティ情報すなわち抽出された情報は、ある基地局から直接別の基地局の転送される。ここで「直接」とは、情報が他の基地局の相互接続バスを構成するネットワークの他の干渉ノードを介して転送される場合でも、抽出された情報の他のソースにアクセスしないことを意味する。好ましいことに単純化されたネットワーク、すなわち制御の観点から回送を低減させたネットワーク、例えばＨＬＲと相互接続を有する基地局ネットワークのみを必要とするネットワークは、性能の劣化を最小に押さえながら、例えばハンドオフプロセスの間、遅延の増加を最小に押さえながら採用される。

【０００８】更に具体的に説明すると、本発明の一実施例においては、ワイヤレス端末からサービスリクエストを最初に受領した第１基地局は、中央セキュリティノード、例えばＨＬＲから認証情報を要求し、それに応答して少なくとも１つ、通常複数のセキュリティ情報を受領する。セキュリティ情報の組は、パスワード、チャレンジー応答対、チャレンジー応答cipher key tuple等である。第１基地局から第２基地局へのハンドオフの時には、第１基地局は第２基地局に中央セキュリティノードから受領したセキュリティ情報の組の少なくとも１つを送る。その後この第２基地局は、第１基地局から受領したこの情報を用いて、ワイヤレス端末を認証するおよび／または暗号化通信に関わる。

【０００９】

【発明の実施の形態】図１は本発明によるネットワーク構成を表す。同図には、（ａ）ワイヤレス端末１０１と、（ｂ）基地局１０３－１から１０３－Ｎを含むＮ個の基地局１０３と、ここでＮは、２以上の整数である、（ｃ）アンテナ１０５－１から１０５－Ｎを含むの個のアンテナ１０５と、（ｄ）構造物１０７－１から１０７－Ｎを含むＮ個の構造物１０７と、（ｅ）セル１０９－１から１０９－Ｎを含むＮ個のセル１０９と、（ｆ）ネットワーク１１１と、（ｇ）基地局認証ユニット１１３と、（ｈ）通信リンク１１５－１から１１５－Ｎを含むＮ個の通信リンク１１５と、（ｉ）通信リンク１１７、通信リンク１２１と、（ｊ）セキュリティセンタ１１９とが示されている。

【００１０】ワイヤレス端末１０１は、複数の基地局と通信でき、この基地局は検出可能な十分な信号強度でもって信号を送信し、ワイヤレス端末１０１の現在の位置で通信できる。十分な強度の信号が特定の基地局に対し検出されると、ワイヤレス端末１０１はその基地局と通信を行う。ワイヤレス端末１０１により採用されたワイヤレス（無線）リンクとプロトコル、すなわちエアインタフェースの種類は、本発明にとって本質的要素をなすものではないが、ワイヤレス端末１０１により採用されるワイヤレスリンクとプロトコルは、基地局１０３に採用されるのと同一のものでなければならないが、当業者の必要により、いかなる種類のものでも良い。

【００１１】ワイヤレス端末１０１は複数の基地局と通信を行うことができる。例えばワイヤレス端末１０１は、単一の受信器であり、ワイヤレス端末１０１が信号を受信すると、それに現在サービスしている基地局との情報交換で占有されていない場合には、ワイヤレス端末１０１に到達するのに十分な強度の信号を有する他の基地局から信号を受信することができる。別の構成例として、ワイヤレス端末１０１は、複数の基地局から同時に、例えばワイヤレス端末１０１内の複数の並列受信器を採用することにより信号を受信することができる。さらにまた別の構成例として、ワイヤレス端末１０１は、複数の受信器であるが、受信器の数はワイヤレス端末１０１が、その現在いる場所で十分な強度の信号を受信できる基地局の数以下であり、その結果ワイヤレス端末１０１は、ある基地局からの信号を得るために、その受信器の少なくとも１つに対し走査を実行する必要がある。

【００１２】基地局１０３は、以下の説明を除いて従来の基地局である。まず第１に基地局１０３は、基地局間通信に対し専用ネットワークに接続される必要はない。その代わりに基地局１０３は、共有公衆ネットワーク、例えばインターネットのようなＩＰベースのネットワークを採用することができる。第２に、各基地局１０３は、「地図」情報を含む必要がない。その代わりに各基地局１０３は、「地図」情報の必要な部分のみを発見することができればよい。好ましくは、基地局１０３は小さなスペースに容易に組み込むことのできる小さな基地局である。例えば、専用の構造およびサイトを準備するのではなく、すでに利用可能なスペースに組み込まれた基地局である。好ましいことにこのような小型化は、「地図」情報の必要な部分を見いだす機能と共に、新たなワイヤレス通信ネットワークの早急な構築が可能となる。さらにまたこのようなワイヤレス通信ネットワークは、そのアーキテクチャーがフレキシブルである、すなわち基地局は容易に追加、あるいは取り外すことができ、そしてさらにはまたそれを維持することも容易である。

【００１３】各アンテナ１０５は、基地局１０３のそれぞれに接続されている。アンテナ１０５は、それぞれの基地局１０３により生成された信号を放射する。基地局１０３の１つとアンテナ１０５とそれに対応する１つの各組合せが、セル１０９の１つを生成する。図１のセル１０９の形状は、実際のセルの形状を示してはおらず、単にセルに対する従来の概念を示したに過ぎない。実際の様々なセル１０９の形状は全て異なる。

【００１４】各構造物１０７は、１つあるいは複数の基地局１０３を配置するための設備を有する。さらにまた構造物１０７は、アンテナ１０５を搭載する場所を提供する。例えばある構造物１０７は、１つの基地局１０３が未使用の場所に配置され、１つのアンテナ１０５が外部から取り付けられる既存の家である。

【００１５】通信リンク１１７は、互いに通信する、および基地局認証ユニット１１３、セキュリティセンタ１１９と通信するための通信路を、基地局１０３に対し提供する。ネットワーク１１１は、様々なサブネットワークから構成される。さらにまた様々なサブネットワークは、異なる種類および異なるプロトコルを採用することも可能である。本発明の一実施例においては、ネットワーク１１１はパケットベースのネットワーク、例えばＡＴＭネットワーク、あるいはＩＰネットワークである。

【００１６】各基地局１０３は、ネットワーク１１１にそれぞれ通信リンク１１５の１つを介して接続される。この通信リンク１１５はネットワーク１１１の一部とみなすことができる。例えば、ネットワーク１１１あるいは少なくともそのサブネットワークはＩＰネットワークであり、１つの基地局１０３は家である構造物１０７内に配置される。通信リンク１１５はインターネット接続であり、例えばケーブルテレビのライン、あるいは家から屋外への接続を介して行われるもので、これは他の基地局との通信を行う基地局により、あるいはインターネットのブラウジングを行うための家の所有者により共有される。

【００１７】基地局認証ユニット１１３は、全て有効な基地局１０３のリストとそれに関連する情報、例えば基地局のセキュリティキーと別の識別子とあるいはアドレスを含む。基地局認証ユニット１１３にあげられた基地

局は、どの地点のものでも良い。しかし基地局は基地局認証ユニット１１３内のリストにあげられた場合のみ有効となる。同図には１つの装置としてしか示していないが、実際には基地局認証ユニット１１３はいくつかのパーツから構成され、これらは必ずしも地理的に同じ場所にある必要はない。さらにまた信頼性および性能を改善するために、基地局認証ユニット１１３の様々なパーツ、あるいは機能の一部あるいはすべてを複製することもできる。

【００１８】基地局認証ユニット１１３はネットワーク１１１に通信リンク１１７を介して接続される。基地局認証ユニット１１３が複数のパーツから構築されている場合、あるいは複製されている場合には、通信リンク１１７は、ネットワーク１１１と様々なパーツとの間の必要な通信バスをカバーするものとして解釈できる。

【００１９】セキュリティセンタ１１９は、サービスされている全ての有効ワイヤレス端末のリストを含む。さらにまた、セキュリティセンタ１１９はセキュリティ情報、例えば認証、チャレンジー応答対および／または各ワイヤレス端末に関連する暗号化キーを含む。セキュリティ情報は、必要によってはセキュリティセンタ１１９により基地局１０３に分配される。ワイヤレス端末はどの場所でも１１０内にリストアップすることができる。しかしワイヤレス端末は、セキュリティセンタ１１９内のリストに載ったとき初めて有効となる。図では１つの装置として示されているが、実際にはセキュリティセンタ１１９は数個のパーツから組み合わされ、これらのパーツは必ずしも地理的に同一場所にある必要はない。さらにまた信頼性と性能を改善するために、セキュリティセンタ１１９の様々なパーツ、あるいは機能の一部、あるいはすべては複製することができる。

【００２０】セキュリティセンタ１１９はネットワーク１１１に通信リンク１２１を介して接続される。セキュリティセンタ１１９が複数のパーツから構築されている場合、あるいは複製されている場合には、通信リンク１２１は、ネットワーク１１１と様々なパーツとの間の必要な通信バスをカバーするものとして解釈できる。

【００２１】図２は、本発明により図１の基地局間のハンドオフを実行するフローチャートを示す。具体的に説明すると、ハンドオフのプロセスの一部として基地局は、基地局の「地図」の少なくとも一部、すなわち近隣の基地局のパターンとそれの関連情報を見いだし更新する。特定の基地局により見いだされた地図の一部は、それがサービスしている呼がハンドオフされる近隣のものである。ローカル地図全体を見いだすために特定の基地局に対する近隣の基地局でもって、少なくとも１回のハンドオフが行われる。

【００２２】本発明のプロセスは、ステップ２０１で開始され、ワイヤレス端末、例えばワイヤレス端末１０１（図１）が、ワイヤレス端末が通信している基地局、例えば基地局１０３－１の無線リンクの信号が、別の基地局、例えば基地局１０３－２のそれよりも弱くなり、この別の基地局がより良好な無線リンクを提供するようになったために、ワイヤレス端末、例えばワイヤレス端末１０１はハンドオフをリクエストする。次に条件ブランチポイント２０３では、第１基地局、例えば基地局１０３－１への接続が存在するか否かを決定する。この理由は、第１基地局から受信した信号がワイヤレス端末で弱くなるか、あるいは第１基地局で受信したワイヤレス端末からの信号が弱くなり、その結果第１基地局とワイヤレス端末との間の接続がハンドオフが行われる前に難しくなるからである。ステップ２０３のテスト結果がＹＥＳの場合は、第１基地局とワイヤレス端末との間の接続が依然と存在していることを示し、制御はステップ２０５に移り、そこでワイヤレス端末は第１基地局から第２基地局、例えば基地局１０３－２へのハンドオフを要求する。別法としてワイヤレス端末は、第１基地局と第２基地局に対するワイヤレス端末で受信した信号強度の様々な測定値を、第１基地局に送り、この第１基地局はハンドオフに適した時間を決定する。そのため第１基地局は、ワイヤレス端末に対し第２基地局に接続するよう指示する。

【００２３】次に条件ブランチポイント２０７は、第１基地局が第２基地局を認識しているか否かを決定する。すなわち第１基地局はその地図情報内にリストアップされている第２基地局を有しているか否かを決定する。このリスティングは、第１基地局と第２基地局の間のワイヤレス端末の前のハンドオフの結果である。具体的に説明すると、地図情報内のリスティングの一部として第１基地局は、（ａ）第２基地局の基地局識別子と、（ｂ）第２基地局のネットワークアドレス、例えばそのＩＰアドレスと、（ｃ）セキュリティ情報、例えば本発明により第１基地局と第２基地局との間の通信を確保するのに用いられる第２基地局のパブリックキーを認識している。２０７のテスト結果がＮＯの場合は、第１基地局は第２基地局を認識せずに制御はステップ２０７に進み、そこで第１基地局はワイヤレス端末に対し、第１基地局は第２基地局を認識せずに、そしてワイヤレス端末はそれ自身の上の第２基地局とのワイヤレスリンク接続をアレンジしなければならない。これは例えば、ワイヤレス端末がその基地局のよりサービスされているセル内で最初に電源が入れられた時に、基地局との初期のワイヤレスリンクを確立するのに、ワイヤレス端末が用いる同一のプロセスを用いることにより行われる。

【００２４】ステップ２０３のテスト結果がＮＯの場合は、ワイヤレス端末から第１基地局への接続が打ち切られるか、あるいはステップ２０９の後制御はステップ２１１に進み、そこでワイヤレス端末は、第２基地局がワイヤレス端末とワイヤレスリンクを確立するようリクエストする。このリクエストに応答して条件ブランチポイ

ント２１２では、第２基地局は、第２基地局が第１基地局を認識しているか否かを決定する。ステップ２１２のテスト結果がＮＯの場合には第２基地局は、第１基地局を認識していないことを示し、制御は２１３に進み、そこで第２基地局は、ワイヤレス端末を認証しようと試みて、この試みでは図１のセキュリティセンタ１１９内に記憶された情報の参照を必要とする。その後制御はステップ２１５に進み、プロセスは以下に説明するよう継続される。ステップ２１２におけるテスト結果がＹＥＳの場合、制御は２１４に進み、そこでワイヤレスに対するセキュリティ情報が第１基地局で要求され、そこから本発明にしたがって第２基地局が受信する。好ましいことに、第１基地局をすでに認識している第２基地局は、セキュリティセンタによるワイヤレス端末の認証に関わる必要はない。このため、ハンドオフプロセスの容易さとかなりの時間が節約できる。通常行われることであるため図２には示してはいないが、第１基地局でセキュリティ情報が得られない場合には、第１基地局が利用できるセキュリティ情報の全てが使用し尽くされ、制御はステップ２１３に進む。

【００２５】ステップ２０７のテスト結果がＹＥＳの場合、基地局は第２基地局を認識していることを示し、制御は条件ブランチポイント２０８に進み、そこでは第１基地局は、第２基地局により用いられるワイヤレス端末に関連するセキュリティ情報が得られるか否かを決定するためにテストする。このようなセキュリティ情報は、チャレンジーレスポンス認証対および／またはワイヤレス端末に関連する暗号化キー等である。ステップ２０８のテスト結果がＮＯの場合は、第１基地局は、第２基地局により使用することのできるワイヤレス端末に関連するセキュリティ情報が得られないことを示し、制御はステップ２０９に進み、プロセスは上記したように継続する。ステップ２０８のテスト結果がＹＥＳの場合には、第１基地局は第２基地局により使用することのできるワイヤレス端末に関連するセキュリティ情報が得られたことを示し、制御はステップ２２１に進み、そこで第１基地局は本発明により、例えば自分自身に調和して利用可能なセキュリティ情報を第２基地局に送る。セキュリティ情報の送信は、第１基地局から第２基地局へのワイヤレス端末のハンドオフのリクエストとして第２基地局では解釈される。好ましいことに、第１基地局によりすでに信頼された第２基地局は、セキュリティセンタとともにワイヤレス端末の認証に関与する必要はなく、このためかなりの時間の節約とハンドオフプロセスを容易にできる。

【００２６】次にステップ２２３において、ワイヤレス端末は、第２基地局がワイヤレス端末とのワイヤレスリンクを確立するよう要求する。その後、あるいはステップ２１４の実行後、制御は条件ブランチポイント２２５に進み、そこでワイヤレス端末は、第１基地局とデータを通信するために、暗号技術を用いているか否かを決定するためにテストする。ステップ２２５のテスト結果がＮＯの場合は、基地局とデータを通信するためにワイヤレス端末は、暗号リンクを使用していないことを表し、制御はステップ２２７に進み、そこで第２基地局はワイヤレス端末を認証するために第１基地局から得たセキュリティ情報を用いる。その後条件ブランチポイント２１５は、ワイヤレス端末が成功裏に認証されたか否かを決定するためにテストする。

【００２７】ステップ２１５のテスト結果がＹＥＳの場合、ワイヤレス端末は、通信するために基地局を用いることが許されたことを示し、制御はステップ２３１に進み、そこでワイヤレス端末は、ユーザトラフィックを第２基地局の搬送するために接続される。その後プロセスは、ステップ２３３で終了する。ステップ２１５のテスト結果がＮＯの場合、ワイヤレス端末は通信用に基地局を利用することが許されないことを示し、制御はステップ２３３に進み、プロセスはそこで終了する。

【００２８】ステップ２２５のテスト結果がＹＥＳの場合、暗号化リンクが基地局とデータを通信するためにワイヤレス端末により使用されていることを示し、制御はステップ２２９に進み、そこでデータプロセスの暗号化と脱暗号化がワイヤレス端末と第２基地局との間で開始される。このための暗号化アルゴリズムが初期化される。ユーザデータがいったん流れ出すと、暗号化あるいは脱暗号化が適宜自動的に行われる。第１基地局から第２基地局へ渡された新たな暗号化キーの暗号化リンクの使用は、ワイヤレス端末を受領するために行われたハンドオフでは関係しなかった基地局のセル内での活性化に基づいて、ワイヤレス端末が認証された後、ワイヤレス端末の直接的な再認証として同じ目的を達成する。

【００２９】次に制御はステップ２３１に進み、そこでワイヤレス端末は、ユーザトラフィックを搬送するために第２基地局に接続される。このステップの一部として、ワイヤレス端末に第１基地局を介してデータが送信されるネットワークの他の部分は、ワイヤレス端末の第２基地局を介して、例えば公知のモバイルインターネットプロトコルの技術を用いて、新たにデータを転送するために指示される。その後プロセスはステップ２３３で終了する。

【００３０】ステップ２０７のテスト結果がＹＥＳの場合、第２基地局は同様に第１基地局を知っており、これは非日常的なエラーの場合では真実ではない。このようなエラーは、実行されるハンドオフに参加するために、第２基地局の拒否により開始され、スムーズには実行されないハンドオフを行うために、ステップ２０９に制御が進むプロセスを必要とする。

【００３１】第１基地局は第２基地局に、第１基地局が最初に受領したセキュリティ情報の全てを送る必要はない。この理由は、第１基地局は、ワイヤレス端末と通信

11

する際にそのセキュリティ情報の一部を用いており、ある種のセキュリティ情報、例えばチャレンジ－応答対、あるいは符号化キーを使用する良好な試作であるセキュリティ攻撃を未然に防ぐのを助ける。さらにまた、第１基地局により得られたセキュリティ情報は、セキュリティセンタあるいは他の別の基地局から得ることもできる。

【図面の簡単な説明】

【図１】本発明によるネットワーク構成を表す図。

【図２】本発明により図１の基地局間でハンドオフを実行するフローチャート図。

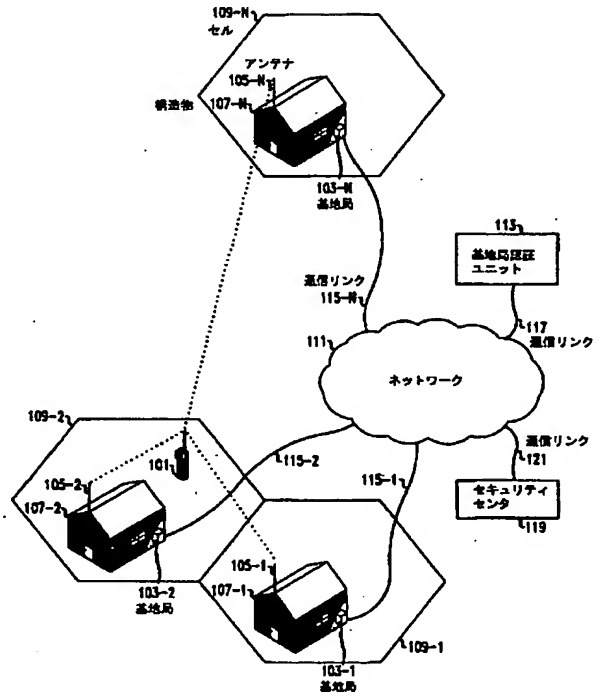
【符号の説明】

１０１　ワイヤレス端末
１０３　基地局
１０５　アンテナ
１０７　構造物
１０９　セル
１１１　ネットワーク
１１３　基地局認証ユニット
１１５、１１７、１２１　通信リンク
１１９　セキュリティセンタ
２０１　開始２０３　第１基地局への接続が存在するか
２０５　ワイヤレス端末は第１基地局から第２基地局へのハンドオフをリクエストする

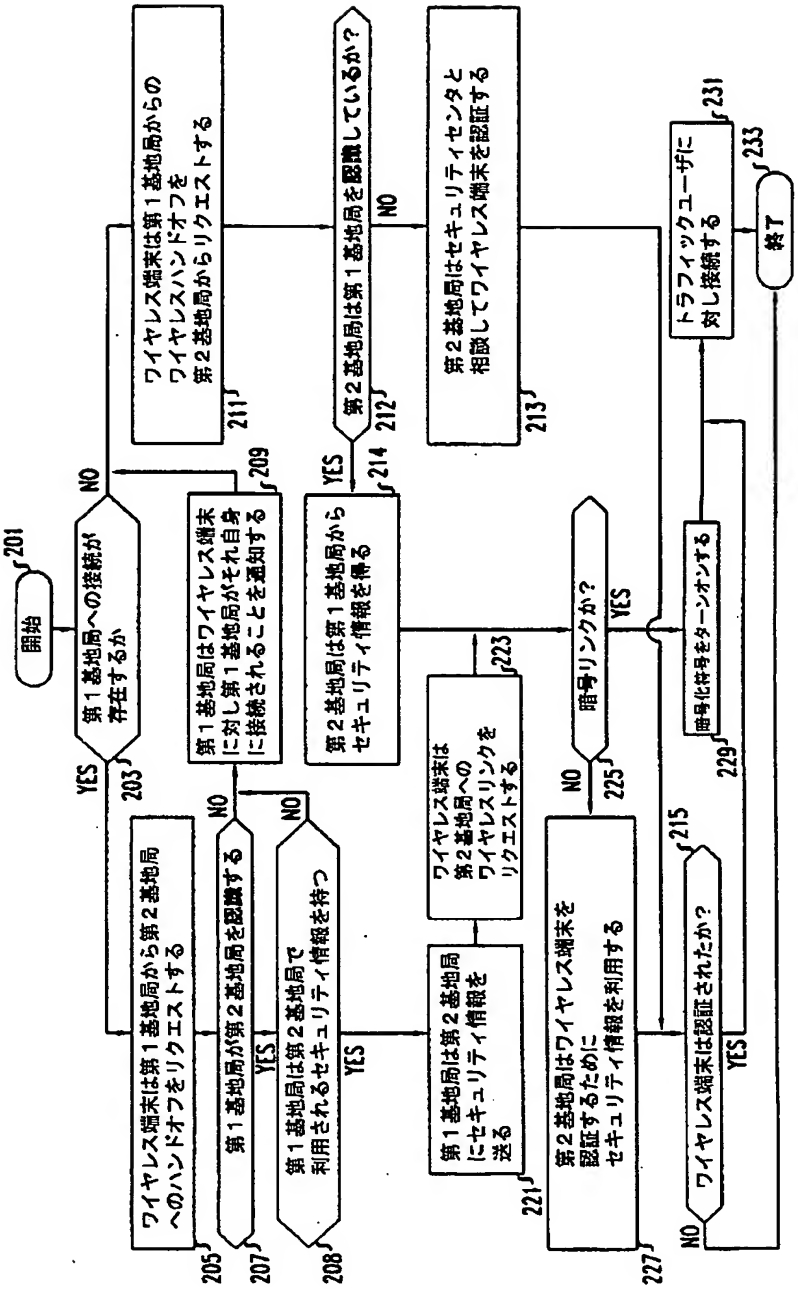
12

＊２０７　第１基地局が第２基地局を認識する
２０８　第１基地局は第２基地局で利用されるセキュリティ情報を持つ
２０９　第１基地局はワイヤレス端末に対し第１基地局がそれ自身に接続されることを通知する
２１１　ワイヤレス端末は第１基地局からのワイヤレスハンドオフを第２基地局からリクエストする
２１２　第２基地局は第１基地局を認識しているか？
２１３　第２基地局はセキュリティセンタと相談してワイヤレス端末を認証する
２１４　第２基地局は第１基地局からセキュリティ情報を得る
２１５　ワイヤレス端末は認証されたか？
２２１　第１基地局は第２基地局にセキュリティ情報を送る
２２３　ワイヤレス端末は第２基地局へのワイヤレスリンクをリクエストする
２２５　暗号リンクか？
２２７　第２基地局はワイヤレス端末を認証するためにセキュリティ情報を利用する
２２９　暗号化符号をターンオンする
２３１　トラフィックユーザに対し接続する
２３３　終了

【図１】



【図２】


開始
201
第１基地局への接続が存在するか
203
YES
NO
ワイヤレス端末は第１基地局からのワイヤレスハンドオフを第２基地局からリクエストする
211
第１基地局はワイヤレス端末に対し第１基地局がそれ自身に接続されることを通知する
209
第２基地局は第１基地局を認識しているか？
212
YES
NO
第２基地局は第１基地局からセキュリティ情報を得る
214
第２基地局はセキュリティセンタと相談してワイヤレス端末を認証する
213
ワイヤレス端末は第１基地局から第２基地局へのハンドオフをリクエストする
205
第１基地局が第２基地局を認識する
207
NO
YES
第１基地局は第２基地局で利用されるセキュリティ情報を持つ
208
NO
YES
第１基地局は第２基地局にセキュリティ情報を送る
221
ワイヤレス端末は第２基地局へのワイヤレスリンクをリクエストする
223
暗号リンクか？
225
NO
YES
第２基地局はワイヤレス端末を認証するためにセキュリティ情報を利用する
227
曲号化符号をターンオンする
229
ワイヤレス端末は認証されたか？
215
NO
YES
トラフィックユーザに対し接続する
231
終了
233

フロントページの続き

(71)出願人 596077259
600 Mountain Avenue, Murray Hill, New Jersey 07974－0636U. S. A.

(72)発明者 ステファン ウィリアム デイビース
カナダ国、Ｍ５Ｓ ２Ｈ９ トロント、スバンディナ アベニュー アパートメント２ 661

(72)発明者 ミカエラ シー、バンダービーン
アメリカ合衆国、07738 ニュージャージー、リンクロフト、ウィロー グローブ ドライブ 114